REMARKS/ARGUMENTS

Claims 1-47 are pending in the present application. Reconsideration of the claims is respectfully requested.

I. Examiner Interview

On July 18, 2007, the examiner and the undersigned attorney discussed the anticipation rejection vis-à-vis claims 1, 30, and 47. No agreement was reached.

II. 35 U.S.C. § 102, Anticipation

The examiner rejected claims 1-47 under 35 U.S.C. § 102 as anticipated by *Ortiz et al.*, Random Biometric Authentication Utilizing Unique Biometric Signatures, U.S. Patent Application Publication No. 2003/0163710, dated December 17, 2002 (hereinafter referred to as *"Ortiz"*). This rejection is respectfully traversed.

Applicants first address the rejection of claim 1. In rejecting claim 1 the Examiner states:

> Regarding Claim 1, *Ortiz* teaches random biometric authentication utilizing unique biometric signatures. The method and associated system for random biometric authentication utilizing unique biometric signatures as taught or suggested by *Ortiz* includes: providing at least a first physical token (¶0067, figure 1, element 44, 'Biometric broker'), the first physical token includes at least one visible characteristic (¶0074, 'This biometric attribute can be any type of biometric measurement of user 33. This includes, but is not limited to, fingerprint data, retinal scan data, handwriting data, voice data (e.g. a voice print), and facial date (e.g. a face scan).'), the first physical token has role information (¶0076, 'Thus biometric authentication can be based on a variety of possible biometric measurements. A user profile 82 of a particular user will thus include one or more of the aforementioned biometric attributes. Such biometric attributes are utilized to verify the identity of the user.") associated therewith, at least one visible characteristic (¶0101, "during another authentication session, the same user can be required to provide a left index fingerprint...") is indicative of at least a first role (¶0101, i.e. "authentication session", ¶0102, i.e. "biometric attributes from the user profile) associated with the first physical token (¶0100, i.e., elements 202 'user interface, 208 'iris scanner', 206 'finger print scanner', etc.); placing the first physical token in a physical relationship with a first computing device (¶0061-0062 and 0067); associating the first computing device with the first physical token (¶0061-¶0062 and 0067); receiving, the first computing device, role information from the first physical token and responsive to the role information being received (¶0061-0062 and 0067-0071), assigning the first role to the first computing device based on the role information (¶0061-0062 and 0067-0071).

Office Action, dated May 02, 2007, pages 1-4.

A prior art reference anticipates the claimed invention under 35 U.S.C. § 102 only if every element of a claimed invention is identically shown in that single reference, arranged as they are in the claims. *In re Bond*, 910 F.2d 831,15 U.S.P.Q.2d 1566, 1567 (Fed.Cir. 1990). All limitations of the claimed invention must be considered when determining patentability. *In re Lowry*, 32 F.3d 1579, 1582, 32 U.S.P.Q.2d 1031, 1034 (Fed.Cir. 1994). Anticipation focuses on whether a claim reads on the product or process a prior art reference discloses, not on what the reference broadly teaches. *Kalman v. Kimberly-Clark Corp.*, 713 F.2d 760, 218 U.S.P.Q. 781 (Fed.Cir. 1983). In this case, *Ortiz* does not identically show each and every feature of the claims.

Claim 1 is as follows:

> 1. A method for assigning a role to a computing device in a network data processing system, the method comprising:
>
> providing at least a first physical token, wherein the first physical token includes at least one visible characteristic, wherein the first physical token has role information associated therewith, and wherein the at least one visible characteristic is indicative of at least a first role associated with the first physical token;
>
> placing at least the first physical token in a physical relationship with a first computing device;
>
> associating the first computing device with the first physical token;
>
> receiving, by the first computing device, the role information from the first physical token; and
>
> responsive to the role information being received, assigning the first role to the first computing device based on the role information.

Applicants first address the rejection with respect to claim 1. *Ortiz* does not anticipate claim 1 because *Ortiz* fails to teach the following features: 1) receiving, by the first computing device, the role information from the first physical token, 2) a physical token that includes at least one visible characteristic that indicates at least a first role associated with the token, and 3) placing at least the first physical token in a physical relationship with a first computing device, as recited in claim 1.

II.1. Receiving the Role Information from the First Physical Token

Ortiz does not teach the claimed feature of a computer device receiving role information from a physical token, as in claim 1. The Examiner asserts otherwise, citing from the following portion of *Ortiz*:

> [0061] Fig. 1 depicts a block diagram illustrating components of an electronic system 12 associated with a database or memory containing biometric attributes 14, in which preferred embodiments of the present invention can be implemented. Database 14 can be linked or integrated with electronic system 12 and can include a at least one user profile 15 containing biometric templates (i.e. samples) of biometric attributes provided previously by particular users. Electronic system 12 can interact with and communicate with a variety of devices and mechanical systems.

[0062] Electronic system 12 can, for example, communicate with a computer workstation 24. In such an example, electronic system 12 can be configured as a remote computer network (e.g. the Internet), or a dedicated computer network (e.g., Intranet, WLAN, LAN, etc.) operating within a particular organization, business, or institution. Electronic system 12 can also be configured to communicate with electromechanical systems, such as entry hardware of a secure building 22. A user can access electronic system 12 to secure entry to secure building 22. In some applications, electronic system 12 can be configured as electronics associated with or resident within the user interface (e.g., typical of non-networked systems, such as secure entries).

[0067] Host systems 48, 40, and 42 can be coupled to biometric broker 44. Biometric broker 44 can be implemented as a centralized repository for storing biometric attributes (i.e., biometric data), such as fingerprint data. Biometric broker 44 can also be configured as an entity that obtains biometric data from a variety of biometric databases operated by different entities and organizations, and utilizes such information for authentication purposes. Fig. 4, which will be further described herein, lists examples of biometric data that can be utilized in accordance with the present invention. Biometric broker 44 can also include a mechanism for managing the biometric attributes stored as data, and can additionally include a mechanism for implementing security policies for the biometric attributes. Such policies can require specific levels of authentication for different groups of users, or for access to different servers.

[0068]Biometric brokers 44 can be implemented in any number of forms. In one possible embodiment, biometric broker 44 can be implemented as a node on network 30, which communicates with host systems 48, 40, and 42 across network 30. In another possible embodiment, biometric broker 44 can be located on a host, such as host system 348.

[0069]The example illustrated in Fig 2. can operate generally as follows. A user, such as user 33, works on a client, such as client system 32. User 33 requests access to resources on host system 48 across network 30. In response to this request, host system 48 attempts to authenticate user 33. In doing so, host system 48 requests a biometric attribute (i.e. biometric data) from biometric broker 44. Biometric broker 44 returns a biometric attribute or biometric template, which can be compared against sample biometric attribute(s) randomly collected from user 33. this comparison can take place at a number of locations, including at client system 32, at host system 38 or at biometric broker 44. If the sample biometric attribute collected from user 33 matches the biometric attribute retrieved from biometric broker 44, user 33 can be permitted to access resources on host system 48.

[0070] Providing a centralized authentication service such as biometric broker 114 has a number of advantages. One advantage is generally that centralized revocation can be supported. For example, an employee in an organization typically has access to a number of different resources on a number of different host systems. When this employee leaves the organization, it often takes a long time to explicitly revoke the employee's access rights on all host systems. Under a centralized revocation scheme, such revocation only needs to take place once at

> the centralized revocation service since the disparate host systems always look to the centralized revocation service to authenticate a user.
>
> [0071] Fig. 3 illustrates a block diagram illustrating some of the functional components within client computer system 32 that can be utilized to implement an embodiment of the present invention. Note that in Figs. 2 and 3 identical parts are represented by identical reference numerals. As mentioned above, client system 32 can be any node on a computer network including computational capability and including a mechanism for communication across network 30. In the illustrated embodiment, client system 32 includes user interface 62, networking code 64 and adapter 66. These functional components can be implemented in software running on, for example, a client CPU. User interface 62 provides a mechanism through which user 33 can operate client system 32. Networking code 64 can include a library of functions, which allow client system 32 to communicate across network 30. Adapter 66 can include a collection of functions that implement the client portion of a biometric authentication system according to one embodiment of the present invention.

Ortiz, page 5, paragraphs 61-62 and 67-71.

The cited portion of *Ortiz* teaches using electronic systems with previously stored data that is associated with the biometric attribute that the user supplies to an electronic system. *Ortiz* discloses a system that then authenticates the user based on this previously stored data and then allows the user access to certain functions or systems.

However, *Ortiz* is not equivalent to the claimed invention. The claimed invention recites receiving role information *from a physical token*. *Ortiz* is not equivalent because a biometric attribute cannot contain, or be made to contain, role information to impart to the computing device. For example, assuming that the biometric attribute that is used to grant a user access is the user's fingerprint, a user's fingerprint cannot transmit any role information to a computer. Rather, the fingerprint is matched to a fingerprint already stored in a database, and *only then* is the user provided with access and other pre-assigned roles on the computing device. Thus, none of the biometric attributes described in *Ortiz* are able to receive role information and then transmit role information to a computing device.

In contrast, the claimed invention recites placing a physical token that *already contains role information* for a computing device that is capable of transmitting role information. Once this physical token is placed in a physical relationship with the computing device, the computing device directly receives role information from this physical token.

As shown above, *Ortiz* does not teach all of the features of claim 1. Therefore, under the standards of *In re Bond*, *Ortiz* does not anticipate the invention of claim 1.

II.2. A Physical Token with At Least One Visible Characteristic wherein the Visible Characteristic is Indicative of Role Information Associated with the Physical Token.

Ortiz does not teach the feature of, "providing at least a first physical token wherein the visible characteristic is indicative of role information associated with the physical token," as in claim 1. The Examiner asserts otherwise, citing the following portion of *Ortiz*:

> [0101] Input of a biometric attribute by a user to interface can be based on the random selection of a biometric attribute from a user profile. The number of biometric attributes requested from a user can also be based on a random number. For example, during one authentication session, a user can be requested to provide a left index fingerprint and a left iris san. During another authentication session, the same user can be required to provide a left index fingerprint, followed by the fingerprint of his or her right middle finger, and immediately thereafter, an iris scan of a left eye, or perhaps, a right eye.
>
> [0102] The selection of biometric attributes from the user profile can thus be based on a random selection. The number of required biometric samples that a user can be required to input can also be a random number. Those skilled in the art will appreciate, however, that the number of biometric attributes required to be input by a user will likely be a limited number. Thus, a user can be required to input only three biometric attributes during one authentication session, two biometric attributes during another authentication session, and five biometric attributes during another biometric session.

Ortiz, page 8, paragraphs 101 and 102.

The cited portion of *Ortiz* discloses authentication sessions, whereby the system asks for a random sampling of biometric attributes from the user to grant access to the system. However, *Ortiz* does not teach a feature that is equivalent to the claimed feature of, "a physical token with at least one visible characteristic, wherein the visible characteristic is indicative of role information associated with the physical token," as in claim 1. For example, the term "visible" in Claim 1 is modifying the word "characteristic" and not the word "token." Claim 1 then goes on to define what a visible characteristic is by stating that the visible characteristic is indicative of at least one role associated with the physical token. *Ortiz* does not disclose such a feature.

By way of illustration only, and without any limitation on the claimed invention, an example of what claim 1 claims could be a key of some sort with a picture of a fax located on said key. This key serves as an example only of a physical token with a visible characteristic that indicates to the user at least one role associated with the physical token. In this example, the fax machine provides a visual clue to the user what role this key serves.

However, in *Ortiz*, the biometric attributes applied to the electronic systems do not have a visible characteristic that indicates visually to the user what role the biometric attribute serves. For example, if the biometric attribute were to be a left index fingerprint or a left iris scan, as is stated in the portions cited

above by the Examiner, no additional visible characteristic on the fingerprint or iris scan is available that indicates to the user of at least one role associated with the biometric attribute. In this case, a specific role cannot be transmitted to the biometric attribute and then received by a computing device from the biometric attribute.

In contrast, the claimed invention teaches providing a physical token where the physical token includes at least one visible characteristic and where the at least one visible characteristic indicates at least one role associated with the physical token. As shown above, *Ortiz* does not disclose using the biometric attributes in the claimed manner. Therefore, under the standards of *In re Bond*, *Ortiz* does not anticipate the claimed invention.

II.3. Placing At Least the First Physical Token in a Physical Relationship with a First Computing Device and Associating the First Computing Device with the Physical Token.

Ortiz fails to teach "placing at least the first physical token in a physical relationship with a first computing device" and then "associating the first computing device with the first physical token." The Examiner asserts otherwise, citing the following portion of *Ortiz:*

> [0061] Fig. 1 depicts a block diagram illustrating components of an electronic system 12 associated with a database or memory containing biometric attributes 14, in which preferred embodiments of the present invention can be implemented. Database 14 can be linked or integrated with electronic system 12 and can include a at least one user profile 15 containing biometric templates (i.e. samples) of biometric attributes provided previously by particular users. Electronic system 12 can interact with and communicate with a variety of devices and mechanical systems.
>
> [0062] Electronic system 12 can, for example, communicate with a computer workstation 24. In such an example, electronic system 12 can be configured as a remote computer network (e.g. the Internet), or a dedicated computer network (e.g., Intranet, WLAN, LAN, etc.) operating within a particular organization, business, or institution. Electronic system 12 can also be configured to communicate with electromechanical systems, such as entry hardware of a secure building 22. A user can access electronic system 12 to secure entry to secure building 22. In some applications, electronic system 12 can be configured as electronics associated with or resident within the user interface (e.g., typical of non-networked systems, such as secure entries).
>
> [0067] Host systems 48, 40, and 42 can be coupled to biometric broker 44. Biometric broker 44 can be implemented as a centralized repository for storing biometric attributes (i.e., biometric data), such as fingerprint data. Biometric broker 44 can also be configured as an entity that obtains biometric data from a variety of biometric databases operated by different entities and organizations, and utilizes such information for authentication purposes. Fig. 4, which will be further described herein, lists examples of biometric data that can be utilized in accordance with the present invention. Biometric broker 44 can also include a

> mechanism for managing the biometric attributes stored as data, and can additionally include a mechanism for implementing security policies for the biometric attributes. Such policies can require specific levels of authentication for different groups of users, or for access to different servers.

Ortiz, page 5, paragraphs 61-62 and 67.

The cited portion of *Ortiz* teaches having electronic systems that register the biometric attributes through their system and a biometric broker that manages the biometric attributes stored as data. *Ortiz* discloses an electronic system that uses biometric attributes to provide authentication to different users and over different servers. *Ortiz* discusses using a fingerprint as the biometric attribute.

However, neither this portion of *Ortiz*, nor any other portion of *Ortiz* teaches the claimed features of, "placing at least the first physical token in a physical relationship with a first computing device" and then "associating the first computing device with the first physical token." For example, the biometric attributes in *Ortiz* cannot be placed in a physical relationship with the electronic system. The biometric broker that stores previously assigned data to an individual user is not able to have a physical relationship with the biometric measurements. A user cannot place their fingerprint in a physical relationship with the computing device and then associate the computing device with their finger. Instead, the user will simply place their finger into a scanning mechanism which will then scan the finger and associate their finger to the computing device.

However, unlike the recited features of claim 1, no actual physical relationship between the finger and the computing device exists in *Ortiz*. In the claimed invention, a direct physical relationship exists because the claimed invention teaches that a physical token is placed in a physical relationship with a computing device and then associated with the computing device.

For example, if the physical token were to be a key of some sort, the claimed invention would provide that this key may then be placed in some sort of physical relationship with the computing device and then left in the computing device in order for the computing device to associate with the key.

However, *Ortiz* does not contain any mention of such a feature as taught by the claimed invention. Therefore, under the standards of *In re Bond, Ortiz* fails to anticipate the claimed invention.

II.4. Remaining Claims

Independent claims 30 and 47 have features similar to those presented in claim 1. Therefore, claims 30 and 47 are distinguishable over *Ortiz* for at least the reasons set forth above.

Claims 2-29, and 31-46 depend on independent claims 1 and 30. Therefore, at least by virtue of their dependency on claims 1 and 30, *Ortiz* does not anticipate these claims.

In addition, dependent claims 2-29 and 31-46 recite additional combinations of features not taught by the cited art. For example, dependent claim 6 recites "wherein the at least one visible

characteristic includes one of a shape, a color, a writing, and visible markings." As discussed above, *Ortiz* does not teach the biometric attribute which contains visible markings that can impart role information to the computing device. Additionally, dependent claim 7 recites, "wherein placing at least the first physical token in a physical relationship with the first computing device includes affixing the first physical token to the first computing device using an adhesive." As discussed above, *Ortiz* neither teaches nor is there a possibility of creating a physical relationship between the biometric attribute and the computing device by affixing the biometric attribute with an adhesive as stated in dependent claim 7. Thus, *Ortiz* fails to disclose the features of dependent claims 6 and 7.

Furthermore, *Ortiz* does not teach, suggest, or give any incentive to make the needed changes to reach the presently claimed invention. Absent the examiner pointing out some teaching or incentive, one of ordinary skill in the art would not be led to modify *Ortiz* to reach the present invention when the reference is examined as a whole. Absent some teaching, suggestion, or incentive to modify *Ortiz* in this manner, the presently claimed invention can be reached only through an improper use of hindsight using Applicants' disclosure as a template to make the necessary changes to reach the claimed invention.

III. Conclusion

The subject application is patentable over the cited references and should now be in condition for allowance. The examiner is invited to call the undersigned at the below-listed telephone number if in the opinion of the examiner such a telephone conference would expedite or aid the prosecution and examination of this application.

DATE: August 1, 2007

Respectfully submitted,

/Theodore D. Fay III/

Theodore D. Fay III
Reg. No. 48,504
Yee & Associates, P.C.
P.O. Box 802333
Dallas, TX 75380
(972) 385-8777
Attorney for Applicants